State of Maine
Department of Administrative & Financial Services
Office of Information Technology

Information Systems Contingency Plan (CP-2)

Table of Contents

1.0 Document Purpose:

The purpose of this document is to describe how the Office of Information Technology (OIT) will assess and recover State of Maine systems hosted by OIT, following a disruption.

2.0 Scope:

2.1 This plan applies to all State of Maine employees and contractors (collectively referred to as personnel in this document) with access to:

2.1.1 Executive Branch Agency *information assets*, irrespective of location; and

2.1.2 Information assets from other State government branches that use the State network.

3.0 Plan Conflict:

If this plan conflicts with any law or union contract in effect, the terms of the existing law or contract prevail.

4.0 Situation:

4.1 OIT provides central leadership and vision in the use of information and telecommunications technology on a statewide basis.

4.2 OIT provides essential technology support and strategic leadership for 12,000 Executive Branch employees, 14 Cabinet-level departments, and all the smaller Executive Branch Agencies. It also provides network support for the Judicial Branch, Secretary of State, and Attorney General.

4.3 OIT also provides technology support to Maine citizens. Examples of this support includes the Maine.gov web portal, the MSCommNet public safety radio communications network, and the ConnectME broadband access expansion.

4.4 In addition to the technology owned and operated by OIT, a number of vendor managed services and systems provide direct support to the groups stated in 4.2 and 4.3.

4.5 Additional situation details can be found in the OIT Cyber Incident Response Plan (coming soon)

5.0 Mission:

5.1 An effective mission statement articulates the primary task and purpose of the plan. The primary task is identified by the fact, if an organization fails to achieve this task, the mission has failed. In this case the key task is conducting persistent *recovery procedures*.

5.2 OIT conducts persistent *recovery procedures* for the data and State of Maine *information assets* that enable the mission and business functions of supported agencies.

6.0 Management Intent:

6.1 The management intent communicates the key tasks and desired end state of the plan to the agency. It is written in such a way the organization can continue with the plan absent continual executive level guidance. It is important that the management intent be written so it can be communicated to anyone involved with the plan.

6.2 The key tasks are the overarching behaviors or actions that management wants everyone to exhibit or complete during all phases of the plan.

6.3 The desired end state articulates what the situation should be after the successful completion of the plan.

6.4 Key to the success of this transition is the following:

6.4.1 The confidentiality, integrity, and availability of the information assets remains the highest priority.

6.4.2 OIT must know the status of information assets on a continuous basis.

6.4.3 OIT must work in cooperation with supported agencies to establish the priority of recovery efforts.

6.4.4 Agencies that contract for vendor managed technology services and assets required by OIT supported agencies must have equivalent recovery procedures for all contracted services.

6.5 Desired end state: OIT maintains essential organizational missions and business functions despite an information asset disruption.

7.0 Constraints:

7.1 Business impact analysis (BIA) and contingency plans (e.g., business continuity plans (BCP)) of supported agencies are in various stages of development.

7.2 Coordination of contingency plan operations as a function of the continuity of government have not been established or exercised.

7.3 The OIT disaster recovery plan (DRP) needs to be created to reflect current-state.

8.0 Facts:

8.1 The Office of Information Technology has finite capacity to recover from disruptions. Recovery from large magnitude outages, such as a disaster, will extend beyond the capacity of OIT, and will require additional resources.

8.2 The scope of a disruption often extends beyond just the assets that OIT is responsible for. This makes the identification of dependencies and coordination with other plans essential.

9.0 Planning Assumptions:

9.1 An outage of a magnitude to be considered a disaster (that is, requires the restoration of essential functions at another location) is handled as a part of the disaster recovery plan (DRP).

9.2 The recovery of information assets because of a cyber incident will be managed as a part the OIT Cyber Incident Response Plan (coming soon)

9.3 As the procedures for the recovery of information assets are developed, they will be added and maintained as a part of this plan.

10.0 Concept of the Operation:

10.1 This contingency plan occurs in four phases. The phases represent a natural progression and subdivision of the plan. These phases should be conceived in condition-driven, rather than time-driven, terms. The intent of each phase to recover information assets to bring the agency back to phase I conditions.

10.2 Phase I- Preparation: OIT is in this phase when the confidentiality, integrity, and availability of the information asset is intact and ends upon notification that an information asset is not available. Generally, the preparation phase includes actions to:

10.2.1 Improve the resiliency of the information asset from an outage

10.2.2 Maintain backups of data to meet recovery objectives

10.2.3 Maintain customer support services to enable the reporting of outages

10.2.4 Improve the contingency plan

10.2.5 Execute the training, testing, and exercises of the plan as outlined in Contingency Plan Training, Testing and Exercise Procedures (IR-2, CP-3, IR-3, and CP-4) (coming soon).

10.3 Phase II- Notification: This phase begins upon notification that an information asset is not available by either external agencies or internal business units responsible for an information asset. The phase ends when procedures to restore an information asset begin. Generally, the notification phase includes actions to:

10.3.1 Continually monitor the availability of assets

10.3.2 Manage customer feedback

10.4 Phase III- Response: This phase begins when procedures to restore an information asset are started and ends with the restoration of the information asset. Generally, the response phase includes actions to recover specific information assets.

10.5 Phase IV- After Actions: This phase begins with the restoration of the information assets and ends with the completion of reporting requirements of the outage. Generally, the after actions phase includes actions to complete:

10.5.1 Reporting requirements of customer support requests

10.5.2 Required after action reporting requirements

10.5.3 Updates to the plan as required

11.0 Procedures:

11.1 **Phase I Preparation:**

11.1.1 OIT Information Security conducts training of contingency plans as outlined in Contingency Plan Training, Testing and Exercise Procedures (IR-2, CP-3, IR-3, and CP-4) (coming soon).

11.1.2 OIT headquarters and both data centers have backup power generators in the event of an outage.

11.1.3 Both data centers have two access points to the internet via the University of Maine.

11.1.4 OIT sections with vendor provided maintenance for IT systems ensure contractual obligations are met and agreements are kept up to date.

11.1.5 Software is updated to the latest supported version.

11.1.6 Infrastructure that provides a redundant capability is maintained at a high state of readiness.

11.1.7 Advanced notification is required when an operating platform is reaching end of life and databases must be moved.

11.1.8 An on-call roster and contact information is posted on the Core Network Status and News (CSN) intranet page. This roster includes the following infrastructure asset owners who are on call after normal business hours to respond to asset outages:

11.1.8.1 Security Infrastructure

11.1.8.2 Network monitoring, Intrusion Detection System (IDS)

11.1.8.3 Network services

11.1.8.4 Voice services, Voice Over IP (VoIP)

11.1.8.5 Data center infrastructure

11.1.8.6 Network Core

11.1.8.7 Wireless

11.1.9 Information asset owners also take actions to prepare for and prevent the occurrence of outages specific to the technologies that they support. A list of information asset owners can be found in Appendix A.

11.1.10 Domain Name Service (DNS): Conducts nightly automated and weekly manual database backups. Failover exercises are conducted as a part of all upgrades.

11.1.11 IT Desktop Support/Field Services: Conducts testing for building outage scenarios. A supply of at least Personal Computers (PCs) are kept in stock to meet emergency needs. The Dell and Hewlett Packard (HP) purchase agreements are maintained to meet additional needs of agency outages.

11.1.12 High Speed Application Printing: Performs regular maintenance of systems to include weekly cleaning.

11.1.13 Enterprise Operations Monitoring (EOM): Maintains documentation in a collaborative manner for the recovery of systems using Wiki pages on Confluence.

11.1.14 Unix: Failover tested during regular patching and storage supports Unix with daily backups.

11.1.15 Firewall: Failover exercised approximately twice per month during standard operation (e.g., routing traffic for Gigamon maintenance).

11.1.16 Remote access/Virtual Private Network (VPN): Create backup images monthly and conduct failover exercises during upgrades.

11.1.17 Network core: Conduct a failover test at inception.

11.1.18 Email (Microsoft Office 365/O365): Maintain three active copies of email located at various datacenters across the country.

11.1.19 SQL Servers / Databases: SQL backups are performed nightly on all databases using an agent from Commvault. SQL Always On is available for databases requiring high availability. SQL Clustering is available for applications requiring high availability and transaction log backups are used, by request, for point in time restores.

11.1.20 Virtual Machine (VM) environment: VM guests are backed up by Commvault. For larger VMs requiring large amounts of RDM (Raw Device Mapping) storage, an iData agent is installed on the server for a full Commvault restore of the VM and storage space. Restores are performed frequently for VM snapshots and with each new operating platform.

11.1.21 Windows servers operating platform: All new servers go through the quality assurance/quality control process which includes checking to see that the server has been added to Commvault backups. The Windows server itself is backed up nightly by Commvault with one full a week and 6 incremental backups. An iData agent from Commvault provides the means to restore a physical server. Restoration is tested on a physical server every time we have a new operating platform.

11.1.22 File and print: Remote file servers are backed up in near real time using CDR (Continuous Data Replication). Backup is done in near real-time by logging all file write activity to a replication log in the source computer, including new files and changes to existing files. The replication log is sent to a CDR server which is then backed up. Commvault backups on file shares are in place for individual file restores on user's shares.

11.1.23 Directory services (Active Directory (AD) and supporting servers): The entire structure is virtual with VM guests being backed up by Commvault. Directory services maintain redundant domain controllers and other support servers (another means of restoring an environment if needed). They also maintain individual restores for Group Policy Objects (GPOs) with AD Tombstone which is available for 180 days.

11.1.24 Storage: Ensures that the scheduled daily, weekly, and monthly backups (both incremental and full) are conducted. Passive hardware presence is maintained to automatically take over in the event of an active failover. Appliances at operating system (OS) levels are kept current. Premium hardware and software support are maintained on all appliances.

11.1.25 Backups: Tape libraries are kept at a current operating system. The media agents for Windows servers have redundancy built-in with three primaries in each data center. Patch maintenance is performed as updates are made available.

11.1.26 Additional details about storage and backup can be found in Media Protection Policy and Procedures (MP-1) (coming soon).

11.2 **Phase II Notification:**

11.2.1 A disruption could be reported by users, external entities (e.g., Multi-State Information Sharing and Analysis Center (MS-ISAC)), 3rd party vendor (e.g., Harris, Microsoft), automated alert (e.g., WebNM), or via automated notification / observation of the technology itself to / by infrastructure asset owners.

11.2.2 Reports from users would most likely go to the OIT Help Desk phone or through a Footprints ticket. The OIT Help Desk would involve the appropriate technicians to remediate the disruption. The OIT Help Desk notifies OIT Information Security if a request is determined to be related to a cyber incident.

11.2.3 After normal business hours, reports from users would most likely go to Enterprise Operations Monitoring (EOM) via the OIT Help Desk phone. EOM notifies on call support to restore systems as required.

11.2.4 For database issues related to physical access the Bureau of General Service (which is the application owner) are notified.

11.2.5 All information assset recovery from notification to after actions is ultimately documented in Footprints.

11.3 **Phase III Response actions:**

11.3.1 The restoration of information assets must occur without the deterioration of the security safeguards originally planned and implemented.

11.3.2 Asset owners typically assess any disruptions and conduct remediation to restore information assets to a fully operational capability. Asset

owners maintain the trained staff and documented procedures specific to the technologies that they support.

11.3.3 Information assets with a redundant capability rely on the available system until the disrupted system is restored.

11.3.4 Information assets with failover capabilities previously described are utilized when the main system fails.

11.3.5 Back-ups and roll-back capabilities may also be leveraged for the restoration of information assets.

11.3.6 Vendor support is utilized as required to restore information assets.

11.3.7 Select hardware may be replaced under either a full or limited warranty.

11.4 **Phase IV After Actions common to all information assets, where applicable:**

11.4.1 Significant incidents require an after action report (see Cyber Incident Reporting Procedures (IR-6), Appendix E "Formal After-Action Review (AAR) Report" (coming soon))

11.4.2 Internal procedures are updated as required. Internal knowledge transfer to team leads and members, including lessons learned occur for unique outages.

11.4.3 Communication of the restoration of information assets are conducted by footprints, email, and CNN.

12.0 Document History and Distribution:

Version	Revision Log	Date
Version 1.0	*Initial Publication*	*August 23, 2019*

Approved by: Chief Information Officer, OIT.

Legal Citation: Title 5, Chapter 163: Office of Information Technology[1].

Distribution

This document will be distributed to all appropriate State of Maine personnel and will be posted on the OIT website (https://www.maine.gov/oit/policies-standards).

[1] http://legislature.maine.gov/statutes/5/title5ch163sec0.html

13.0 Document Review:

This document is to be reviewed annually and when substantive changes are made to policies, procedures or other authoritative regulations affecting this document.

14.0 Records Management:

Office of Information Technology security policies, plans, and procedures fall under the *Routine Administrative Policies and Procedures and Internal Control Policies and Directives* records management categories. They will be retained for three (3) years and then destroyed in accordance with guidance provided by Maine State Archives. Retention of these documents will be subject to any future State Archives General Schedule revisions that cover these categories.

15.0 Public Records Exceptions:

Under the Maine Freedom of Access Act, certain public records exceptions may limit disclosure of agency records related to information technology infrastructure and systems, as well as security plans, procedures or risk assessments. Information contained in these records may be disclosed to the Legislature or, in the case of a political or administrative subdivision, to municipal officials or board members under conditions that protect the information from further disclosure. Any aggrieved person seeking relief for an alleged violation of the FOAA may bring suit in any Superior Court in the state.

16.0 Definitions:

16.1 **Information Asset**: Used interchangeably with **Information System**. A discrete, identifiable piece of information technology, including hardware, software, and firmware. Information assets include, for example, mainframes, workstations, servers (e.g., database, electronic mail, authentication, web, proxy, file, domain name), input/output devices (e.g., scanners, copiers, printers), network components (e.g., firewalls, routers, gateways, voice and data switches, process controllers, wireless access points, network appliances, sensors), operating systems, virtual machines, middleware, business applications, system software, development tools, and miscellaneous related utilities.

16.2 **Recovery Procedures:** Actions necessary to restore data files of an information system and computational capability after a system failure. SOURCE: CNSSI-4009.

Appendix A – Information Asset Ownership

Owner	Information Asset
Application Development Managers	Business Applications
Client Technologies	Enterprise Operations Monitoring (EOM)
	FirstNet
	High Speed Application Printing
	IT Desktop Support/Field Services
	IT Radio Operations (MSCommNet)
Computing Infrastructure and Services	Backups
	Directory services (Active Directory and supporting servers)
	Email (Microsoft Office 365/O365)
	File and print
	SQL servers: SQL databases
	Storage
	Virtual Machine (VM) environment
	Windows servers operating platform
Enterprise Data Services	Oracle Database, Oracle Middleware
	Unix
Information Security Office	Network monitoring, Intrusion Detection System (IDS)
	Physical Access (Badges)
	Security Infrastructure
Network and Data Center	Data center infrastructure
	Domain Name Service (DNS)
	Firewall
	Network core
	Network services
	Remote access/Virtual Private Network (VPN)
	Voice services, Voice Over IP (VoIP)
	Web Application Firewall (WAF), Distributed Denial of Service (DDoS) protection, Reverse Proxy
Network and Data Center	Wireless